REMARKS

Claims 1-3, 5-24, 26-28, 50-51 and 53-68 are pending in the present application. Claims 59 and 63 have been amended. Applicants respectfully request allowance of the present application in view of the arguments set forth herein below.

The amendments to claims 59 and 63 are simply for the purpose of clarification in view of the amendments filed with the RCE.

Claim Rejections – 35 USC § 103

The Office Action rejected claims 1-3, 5-9, 11-14, 16-24, 26-28, 50, 51 and 53-68 under 35 U.S.C. §103(a) as being allegedly obvious over various references. These rejections are respectfully traversed in their entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Any differences between the prior art and the claims at issue must be such that they would have been obvious to a person having ordinary skill in the art at the time the invention was made. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 167 L.Ed.2d 705, 75 USLW 4289, 82 U.S.P.Q.2d 1385 (2007). Furthermore, the reason that would have prompted the combination of prior art references or the modification of a prior art reference must be found in the prior art, common knowledge, or the nature of the problem itself, and not based on the Applicant's disclosure. *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1367 (Fed. Cir. 2006); MPEP § 2144. Indeed, underlying the obvious determination is the fact that statutorily prohibited hindsight must not be used. *KSR*, 127 S.Ct. at 1742; *DyStar*, 464 F.3d at 1367.

In applying references, "it is necessary to properly construe what an applied reference *fairly* teaches or discloses." *See, e.g., In re Fracalossi and Wajer*, 681 F.2d 792 (CCPA 1982)

(reference is prior art not only for specifically disclosed embodiments, but also all that it fairly teaches). The Examiner, however, cannot arbitrarily import subject matter that is not part of the references relied upon in order to justify a rejection. *See, e.g., Ex Parte Williams* at p. 5, Decision on Appeal in App. No. 11/275,039, BPAI (Feb 24, 2010) (drawing an imaginary line through an arbitrary location on a disclosed seat foam pad as a line of demarcation between the headrest portion and the backrest portion, which forms the basis for the Examiner's finding of anticipation, is contrary to the explicit teachings of the reference patent and not within the realm of what the reference reasonably and fairly teaches).

Claims 50 and 56

The Office Action rejected claims 50 and 56 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."). These rejections are respectfully traversed in their entirety.

Applicants respectfully submit that claims 50 and 56 are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al. with Kurn et al. fails to teach or suggest all of the limitations of claims 50 and 56, and one of ordinary skill in the art would not arrive at the limitations of claims 50 and 56 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management. Arthan et al. teaches a private key and public key pair where the private key is encrypted for delivery using a key encryption key (KEK) and stored in an encrypted state at a source computer 1, where it is decrypted whenever it is needed for use in the transmission of data. See *Arthan et al.* at col. 2, lines 40-48. Arthan et al. suggests that a source system 1 uses a private key (DSPR) to protect data flowing from the source system 1 to a destination system 2. *Id.* at col. 1, lines 58-67. Arthan et al. discloses that the source system 1 and the destination system 2 can actually comprise a large number of physically separate nodes which are attached via a wide area network. *Id.* at col. 2, lines 30-34. The architecture of central system 5 is not specifically

defined, except where the only figure, FIG. 1, illustrates the central system 5 as a separate and distinct entity from both the source system 1 and the destination system 2. *See Id.* at FIG. 1.

Arthan et al. teaches that a central system 5 generates private and public keys. *Id.* at col. 3, lines 38-41. After the keys are generated, the private key (DSPR) is transmitted from the central system 5 to the source system 1, and the corresponding public key (DSPU) is transmitted from the central system 5 to the destination system 2. *Id.* at col. 3, lines 25-41. The destination system 2 can also be supplied in advance with a spare version of the public key. *Id.* at col. 4, lines 15-20. When the private key needs to be changed, such as in the event of a compromise, the version of the private key corresponding to the spare public key can be put into immediate use in the source system 1 as soon as it is supplied. *Id.* at col. 4, lines 20-23. Since the public and private keys are generated in pairs, the spare private key corresponding to the spare public key will "need to be held securely after generation and then called up as required." *Id.* at col. 4, lines 25-32.

Notably, there is no disclosure in Arthan et al. indicating that the central system 5 can be integrated into the source system 1 as a physical node of the source system 1. Instead, Arthan et al. illustrates the central system 5 as a separate and distinct entity from the source system 1 and the destination system 2.

Kurn et al. (U.S. Publication No. 2002/0071561) – discloses a method and apparatus for enforcing the separation of computer operations and business management roles in a cryptographic system. According to Kurn et al., a key repository process 20 stores one or more entries defining Operators and two or more entries defining Owners in a database 30. *Kurn et al.* at ¶ [0076]. An integrity key 22 is configured to ensure the integrity of sensitive information within the database 30. *Id.* Each Owner entry retains a share of a protection key 24 configured to protect sensitive information on the database 30. *Id.* The database 30 also stores enterprise credentials 32. *Id.* Crucial information in the database 30 is protected against modification by the integrity key 22, while confidential data is protected by the protection key 24. *Id.* at ¶ [0091]. When the key repository process 20 is restarted, an operator known to the system exposes the integrity key 22 by use of the correct identity and password. *Id.* The protection key 24 is assembled from a set of secrets that are split among the multiple Owners. *Id.* When the requisite

number of Owners have exposed their share of the split protection key 24, the protection key can be recovered. *Id.*

B. Differences Between Claimed Invention and Prior Art

In rejecting claim 50, the Office Action takes the position that the source system 1 and the central system 5 are integrated into a single system or device. *See Office Action* at p. 2. In support of this position, the Office Action cites to Arthan et al. where it discloses "the source system or destination system may actually comprise a large number of physically separate nodes which are attached via a wide area network." *See Arthan et al.* col. 2, lines 32-34, referenced by the *Office Action* at p. 2. The Office Action then makes the assumption that the central system 5 is a node of the distributed source system and, therefore, the central system 5 is just a smaller part of the source system 1. *See Office Action* at p. 2.

The assertion that the central system 5 can be readily integrated into the source system 1, and that such integration would have been obvious is well beyond the realm of what Arthan et al. reasonably and fairly teaches, and is contrary to the explicit teachings of Arthan et al. Indeed, the only motivation to arbitrarily modify Arthan et al. in the manner asserted is strictly based on impermissible hindsight.

As noted, Arthan et al. discloses that "the source and destination systems may each be complex distributed systems ... compris[ing] a large number of physically separate nodes which are attached via a wide area network." *Arthan et al.* at col. 2, lines 31-34. However, the disclosure relating to the architecture in Arthan et al. ends there. In fact, Arthan et al. does not include any disclosure suggesting an integrated relationship, or even the possibility of an integrated relationship between the source system 1 and the central system 5. That is, Arthan et al. is completely devoid of any teaching or suggestion that the central system 5 can be modified to be one of the physically separate nodes constituting the source system 1. As a result, the assertion that the central system 5 is implemented as a physically separate node of the source system 1 finds no support in any of the teachings or suggestions in Arthan et al. Instead, such a modification is only possible as a result of a completely arbitrary and unsupported redesign of the architecture depicted throughout Arthan et al.

In addition to a complete lack of teachings or suggestions supporting the asserted modification, Arthan et al. actually suggests that the source system 1 and the central system 5 are separate and distinct entities. For example, not only does Arthan et al. not suggest that the central system 5 be integrated into the source system 1, the only figure included with the disclosure expressly depicts the source system 1, the destination system 2 and the central system 5 as distinct and separate devices. This separate and distinct architecture depicted in FIG 1 is expressly referred to by the disclosure when stating that the source system 1 can be made up of a large number of physically separate nodes. In other words, even though the disclosure states that the single computer shown in FIG. 1 as the source system 1 can be made up of a large number of physically separate nodes, the figure referred to when making this suggestion expressly shows that the central system 5 is a separate entity from the source system 1. Thus, the FIG. 1 suggests that even though the source system 1 can be made up of a large number of physically separate nodes, Arthan et al. intended and expressly suggests that the central system 5 is a physically separate and distinct entity from the source system 1.

Moreover, mischaracterizing central system 5 as being integrated into the source system 1 renders some of the Arthan et al. disclosure obsolete. For example, Arthan et al. teaches that the private key DSPR is transmitted to the source system 1 from the central system 5, and must be transmitted in a secure manner, such as by using KEK. *See Arthan et al.* at col. 3, lines 25-43. Applicants note that it is unnecessary and superfluous to transmit the private key DSPR from the central system 5 to the source system 1 if the central system 5 is part of the source system 1. Instead, the very suggestion in Arthan et al. that the central system 5 is required to transmit the key material to the source system 1, and use adequately secure means for the transmissions suggests that the central system 5 is separate and distinct from the source system 1. Otherwise, there would be no need to transmit keys to the source system 1 if those keys were already held by the source system 1.

Because Arthan et al. provides no support for the modifications asserted by the Office Action, and because the disclosure instead suggests that the entities are separate and distinct, the proposed modifications are purely arbitrary. For instance, if such modifications were allowable in view of the disclosure, it would also be equally as reasonable to combine the source system 1 and destination system 2 into a single device, to combine the central system 5 and the destination

system 2 into a single device, or even to combine the source system 1, the destination system 2 and the central system 5 into one single device. However, the Office Action arbitrarily selects to combine only the source system 1 and the central system 5 into a single device. The only reason for such an arbitrary modification, which is contrary to the explicit teachings of the reference and far beyond the realm of what the reference reasonably and fairly teaches, is based solely on Applicants' disclosure. As a result, the modification is based solely on the use of statutorily prohibited hindsight.

Further considering the disclosure of Arthan et al. as a whole, the reference actually teaches away from the modifications proposed by the Office Action. For example, by integrating the central system 5 into the source system 1, the security officer 6, who uses the central system 5 to manage the security keys, would become an operator 3 of the source system 1 (e.g., he would become an operator of one of the nodes of the source system). Such a modification, however, is contrary to the express requirements taught in Arthan et al.

For instance, Arthan et al. states that it is "assumed that the example system is such that operators 3 of the source system 1 **are not authorized to handle the private key DSPR itself**." *Arthan et al.* at col. 2, lines 35-38 (emphasis added). However, Arthan et al. also teaches that the management of all keys is under control of a security officer, who uses automated or manual procedures and protocols to arrange for delivery and installation of key material (*Id.* at col. 1, lines 46-50), and that "the security officer can change to the version of DSPR corresponding to the spare DSPU key" (*Id.* at col. 5, lines 7-10). Thus Arthan et al. suggests that the security officer 6 is authorized to handle the private key DSPR in order to manually deliver and install the keys as well as to change the version of the DSPR and cannot, therefore, be an operator 3 who is not authorized to handle the private key DSPR. That is, since the operators 3 of the source system 1 are expressly not authorized to handle the private key DSPR, and the security office 6 is expressly authorized to handle the private key DSPR, the security officer 6 cannot be an operator 3 of the source system 1. Because the security officer 6 cannot become an operator 3 of the source system 1, the central system 5, which the security officer 6 uses to manage the keys, cannot be arbitrarily transformed into a part of the source system 1 without departing from the express requirements of the Arthan et al. disclosure. Thus, according to Arthan et al., a distributed source system 1 must be made up of physical nodes that are each separate and

distinct from the central system 5, which is directly opposed to the modifications suggested by the Office Action.

When Arthan et al. is characterized according to what is reasonably and fairly taught by the disclosure as a whole, Arthan et al. fails to teach or suggest all of the features recited by independent claim 50. Claim 50 recites, "a processor configured to: generate a first private key and corresponding first public key; generate a second private key associated with the first private key; and create a second public key corresponding to the second private key; a storage medium coupled to the processor, the storage medium configured to store the first private key; and a transmitter coupled to the processor to: output the second private key such that it is not stored in the storage medium, the second private key being output as a plurality of shares to a plurality of different entities once, such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; and output the first public key and the second public key to a verifier device; wherein the processor uses the stored first private key for authentication of the mobile user device prior to using the second private key."

As set forth in the Request for Continued Examination filed March 14, 2011, neither of the separate and distinct source system 1, destination system 2 or central system 5 of Arthan et al. is taught as including all of the features recited by independent claim 50.

For example, the central system 5 generates an active private and public key pair and a spare private and public key pair. See *Arthan et al.* at col. 3, lines 38-41; and col. 4, lines 15-20. The central system 5 then outputs the active private key to the source system 1, and the active public key and spare public key to the destination system 2. *Id.* at col. 3, lines 25-41; col. 4, lines 15-20. It appears from Arthan et al. that the central system 5 securely stores the spare private key for future deployment to the source system 1. *Id.* at col. 4, lines 25-32.

Given such teachings by Arthan et al., the central system 5 is contrary in some respects to the device recited in independent claim 50. For example, the central system 5 generates the active private key, and then outputs the active private key to the source system 1 for active use. This is exactly opposite to claim 50, where the processor uses the stored first private key for authentication of the mobile user device. In other words, the central system 5 outputs the active private key, which is then used before the spare private key, while the device of claim 50 stores

the first private key and uses the stored first private key for authentication before using the output second private key.

Another difference is the fact that the central system 5 does not appear to use any of the keys for authentication of the central system 5. Instead, it just generates the keys and then sends them off to other devices for use by these other devices. In view of the forgoing, central system 5 fails to include "a storage medium coupled to the processor, the storage medium configured to **store the first private key**; and a transmitter coupled to the processor to: **output the second private key** such that it is not stored in the storage medium ... wherein the processor **uses the stored first private key for authentication** of the mobile user device **prior to using the second private key**," as recited in independent claim 50.

Turning to the source system 1, Arthan et al. suggests that the source system 1 simply receives the active private key from the central system 5 (*Id.* at col. 3, lines 25-41; col. 4, lines 15-20) and stores the private key into a volatile memory for use (*Id.* at col. 2, lines 48-50). This source system 1 also fails to include all of the limitation of independent claim 50. For example, the source system 1 fails to include a processor configured to generate any keys, or a transmitter coupled to the processor to "output [a] second private key such that it is not stored in the storage medium."

Turning to the destination system 2, Arthan et al. suggests that the destination system 2 simply receives the public keys from the central system 5. Among other features (e.g., generating keys, etc.), the destination system 2 does not appear to store a private key, output a private key, or use a private key.

Accordingly, when Arthan et al. is characterized according to what is reasonably and fairly taught by the disclosure as a whole, none of the separate and distinct entities in Arthan et al. includes a storage medium configured to "**store the first private key**"; a transmitter to "**output the second private key** such that it is not stored in the storage medium," and a processor that "**uses the stored first private key for authentication** of the mobile user device prior to using the second private key."

The Office Action further argues that "a modification decreasing the pieces of hardware (e.g., having one piece of hardware perform the task previously performed by two) is analogous to making functions, structures, or actions integral ... and that it would have been obvious to one

having ordinary skill in the art to make the element integral." *Office Action* at p. 3. However, such modifications are patentable where the recited claims show insight that was contrary to the understanding and expectations of the art. *See MPEP* § 2144.04(V)(B); and *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983). As previously set forth, Arthan et al. expresses the requirement that the operators 3 of the source system 1 are not authorized to handle the private key DSPR itself." *Arthan et al.* at col. 2, lines 35-38. Arthan et al. also teaches that the management of all keys is under control of a security officer, who uses automated or manual procedures and protocols to arrange for delivery and installation of key material (*Id.* at col. 1, lines 46-50), and that "the security officer can change to the version of DSPR corresponding to the spare DSPU key" (*Id.* at col. 5, lines 7-10). Thus, Arthan et al. suggests the need of a security officer 6 authorized to handle private keys in order to manually deliver and install the keys, as well as to change the version of the private keys, while operators 3 of the source system 1 are prohibited from handling the private keys. Combining the central system 5 with the source system 1 such that the user of the integrated device may both operate the device and manage keys was expressly contrary to the understanding and expectations of Arthan et al. Accordingly, modifying Arthan et al. so that the central system 5 and the source system 1 are an integral element would constitute a patentable modification.

Considering Kurn et al., the reference fails to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al. and Kurn et al., when combined, do not teach or suggest at least "a storage medium coupled to the processor, the storage medium configured to **store the first private key**; and a transmitter coupled to the processor to: **output the second private key** such that it is not stored in the storage medium, the second private key being output as a plurality of shares to a plurality of different entities once, such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; ... wherein the processor **uses the stored first private key** for authentication of the mobile user device **prior to using the second private key**," as recited in independent claim 50, and these differences between claim 50 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was

made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 50.

Furthermore, the nonobviousness of independent claim 50 precludes a rejection of claim 56, which depends therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 56, in addition to the rejection to independent claim 50.

Claims 1-3, 5-9, 11-14, 16-24, 26-28, 51, 53-55 and 57-68

The Office Action rejected claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."), and further in view of U.S. Publication No. 2002/0018570 (hereinafter "Hansmann et al."). These rejections are respectfully traversed in their entirety.

Applicants respectfully submit that claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al., Kurn et al. and Hansmann et al. fails to teach or suggest all of the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55, and one of ordinary skill in the art would not arrive at the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management, as summarized hereinabove with reference to the rejections of claims 50 and 56.

Kurn et al. (U.S. Publication No. 2002/0071561) – discloses a method and apparatus for enforcing the separation of computer operations and business management roles in a cryptographic system, as summarized hereinabove with reference to the rejections of claims 50 and 56.

Hansmann et al. (U.S. Publication No. 2002/0018570) – discloses a simplified authentication system for communicating devices having fewer security requirements than conventional cryptographic systems. *Hansmann et al.* at Abstract. The device to be authenticated includes a secret, a function component for generating a random number, a function component for exchanging messages with other devices and finally an algorithm for calculating a hash using the random number and secret. *Id.* The device requesting authentication includes a secret and an algorithm for calculating a hash using a random number received from the device to be authenticated. *Id.* A function component for comparing both hashes may be implemented in both devices. *Id.* If the hashes calculated by both devices match, it can be assumed that the authentication was successful. *Id.* Instead of using the digital keys and conventional symmetric or asymmetric algorithms, Hansmann et al. contemplates using a relatively simple random number and a simple hash algorithm, which sufficiently fulfills the security requirements of many communication architectures. *Id.*

B. Differences Between Claimed Invention and Prior Art

Claims 1-3, 5-9, 14, 16-18, 22-24 and 53-55

Claim 1 recites in part "outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible; transmitting the first public key and the second public key to a verifier device; and using the retained first private key for authentication of the mobile user device prior to using the second private key."

The rejection of claim 1 is dependent upon the same arbitrary modification of Arthan et al. as asserted against independent claim 50. Specifically, the Office Action takes the position that the source system 1 and the central system 5 are integrated into a single system or device. *See Office Action* at p. 2. However, as noted above, the characterization of Arthan et al. as teaching that the central system 5 can be readily integrated into the source system 1, and that

such integration would have been obvious is well beyond the realm of what Arthan et al. reasonably and fairly teaches, and is contrary to the explicit teachings of Arthan et al. Indeed, the only motivation to arbitrarily modify Arthan et al. in the manner asserted is strictly based on impermissible hindsight.

For instance, there is no teaching or suggestion that the central system 5 is or can be implemented as a physically separate node of the source system 1. Instead, throughout the disclosure, Arthan et al. actually depicts and suggests that the source system 1 and the central system 5 are separate and distinct entities. Furthermore, the mischaracterization of the central system 5 being integrated into the source system 1 renders various teachings in Arthan et al. as obsolete and meaningless. Indeed, the arbitrary modification of Arthan et al. is based solely on Applicants' disclosure, as a result of statutorily prohibited hindsight.

Additionally, Arthan et al., when considered as a whole, teaches away from the modifications proposed by the Office Action. For instance, Arthan et al. expressly requires that the operators 3 of the source system 1 are not authorized to handle the private key. *Arthan et al.* at col. 2, lines 35-38. On the other hand, the security officer 6 is suggested as being authorized to handle the private key in order to manually deliver and install the keys, and to change the various versions of the private key. *Id.* at col. 1, lines 46-50; and col. 5, lines 7-10. Thus, the security officer 6 cannot become an operator 3 of the source system 1. Therefore, the central system 5, which the security officer 6 uses to manage the keys, cannot be arbitrarily transformed into a part of the source system 1 without departing from the express requirements of the Arthan et al. disclosure.

Furthermore, the fact that Arthan et al. suggests that the security officer 6, who uses the central system 5 to manage the private keys, cannot be an operator 3 of the source system 1 is evidence supporting the conclusion that the proposed modification of Arthan et al. would not be obvious, but would instead be patentable. That is, combining the central system 5 with the source system 1 such that the user of the integrated device may both operate the device and manage keys is expressly contrary to the understanding and expectations of Arthan et al., and such modifications are patentable when they show insight that was contrary to the understanding and expectations of the art. *See MPEP* § 2144.04(V)(B); and *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983).

Finally, when Arthan et al. is characterized according to what is reasonably and fairly taught by the disclosure as a whole, Arthan et al. fails to teach or suggest all of the features recited by independent claims 1, 14 and 22, since neither of the separate and distinct entities from among the source system 1, destination system 2 or central system 5 are taught or suggested by Arthan et al. as including all of the features recited by independent claims 1, 14 and 22.

For instance, as noted above regarding independent claim 50, the central system 5 of Arthan et al. generates an active private and public key pair and a spare private and public key pair. See *Arthan et al.* at col. 3, lines 38-41; and col. 4, lines 15-20. The central system 5 then outputs the active private key to the source system 1, and the active public key and spare public key to the destination system 2. *Id.* at col. 3, lines 25-41; col. 4, lines 15-20. It appears from Arthan et al. that the central system securely stores the spare private key for future deployment to the source system 1. *Id.* at col. 4, lines 25-32.

Such a central system 5 is contrary in at least some respects to the recitations in independent claim 1. In claim 1, the **retained** private key is used for authentication prior to using the output private key. In the central system 5, the **output** private key is used by the source system 1 prior to using the stored spare private key.

In addition, the central system 5 that creates the first and second key pairs does not appear to actually use any of the keys for authentication of the central system 5. Instead, it just generates the keys and then sends them off to other devices for use by these other devices. This is contrary to claim 1, where the first and second private keys and first and second public keys are created at the mobile user device, and the retained first private key is used for authentication of the mobile user device.

Arthan et al. also does not teach or suggest the source system 1 or the destination system 2 as performing any steps relating to outputting one private key while retaining another private key and using the retained private key for authentication. Accordingly, Arthan et al. fails to teach of suggest "**outputting the second private key** from the mobile user device such that it is not stored on the mobile user device **while retaining the first private key** in the mobile user device," and "**using the retained first private key** for authentication of the mobile user device **prior to using the second private key**," as recited in independent claim 1.

Furthermore, neither Kurn et al. nor Hansmann et al. include any teachings or suggestions to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "**outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device**, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible; transmitting the first public key and the second public key to a verifier device; and **using the retained first private key for authentication** of the mobile user device **prior to using the second private key**," as recited in independent claim 1 and as similarly recited in independent claim 14, and these differences between claims 1 and 14 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 1 and 14.

Similarly, Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "**retain the first private key and output the second private key** such that it is not stored on a device where the second private key was created, the second private key being output as a plurality of shares to a plurality of different entities once such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; output the first public key and the second public key to a verifier device; and **use the retained first private key for authentication prior to using the second private key for authentication**," as recited in independent claim 22, and these differences between claim 22 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 22.

Furthermore, the nonobviousness of independent claims 1, 14 and 22 precludes a rejection of claims 2, 3, 5-10, 15-18, 23, 24 and 53-55, which depend therefrom, because a

dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 2, 3, 5-10, 15-18, 23, 24 and 53-55, in addition to the rejection to independent claims 1, 14 and 22.

Claims 11-13, 19-21, 26-28 and 51

Claim 11 recites, "receiving a first public key from a mobile user device **wherein the first public key has a corresponding first private key stored on the mobile user device**; receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication; **using the first public key for authentication** of the mobile user device; and **using the second public key for authentication if the first public key fails**."

Similar to the rejections of independent claims 1, 14, 22 and 50, the rejections of independent claims 11, 19, 26 and 51 are dependent on the same arbitrary modification of Arthan et al. consisting of integrating the central system 5 into the source system 1 to obtain a single system or device.

However, as noted above with regards to independent claim 50, the characterization of Arthan et al. as teaching that the central system 5 can be readily integrated into the source system 1, and that such integration would have been obvious is well beyond the realm of what Arthan et al. reasonably and fairly teaches, and is contrary to the explicit teachings of Arthan et al. Indeed, the only motivation to arbitrarily modify Arthan et al. in the manner asserted is strictly based on impermissible hindsight.

For instance, there is no teaching or suggestion that the central system 5 is or can be implemented as a physically separate node of the source system 1. Instead, throughout the

disclosure, Arthan et al. actually depicts and suggests that the source system 1 and the central system 5 are separate and distinct entities. Furthermore, the mischaracterization of the central system 5 being integrated into the source system 1 renders various teachings in Arthan et al. as obsolete and meaningless. Indeed, the arbitrary modification of Arthan et al. is based solely on Applicants' disclosure, as a result of statutorily prohibited hindsight.

Additionally, Arthan et al., when considered as a whole, teaches away from the modifications proposed by the Office Action. For instance, Arthan et al. expressly requires that the operators 3 of the source system 1 are not authorized to handle the private key. *Arthan et al.* at col. 2, lines 35-38. On the other hand, the security officer 6 is suggested as being authorized to handle the private key in order to manually deliver and install the keys, and to change the various versions of the private key. *Id.* at col. 1, lines 46-50; and col. 5, lines 7-10. Thus, the security officer 6 cannot become an operator 3 of the source system 1, and the central system 5, which the security officer 6 uses to manage the keys, cannot be arbitrarily transformed into a part of the source system 1 without departing from the express requirements of the Arthan et al. disclosure.

Furthermore, the fact that Arthan et al. suggests that the security officer 6, who uses the central system 5 to manage the private keys, cannot be an operator 3 of the source system 1 is evidence supporting the conclusion that the proposed modification of Arthan et al. would not be obvious, but would instead be patentable. In other words, combining the central system 5 with the source system 1 such that the user of the integrated device may both operate the device and manage keys is expressly contrary to the understanding and expectations of Arthan et al., and such modifications are patentable when they show insight that was contrary to the understanding and expectations of the art. *See MPEP* § 2144.04(V)(B); and *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983).

Finally, when Arthan et al. is characterized according to what is reasonably and fairly taught by the disclosure as a whole, Arthan et al. fails to teach or suggest all of the features recited by independent claims 11, 19, 26 and 51, since neither of the separate and distinct entities from among the source system 1, destination system 2 or central system 5 are taught or suggested by Arthan et al. as including all of the features recited by independent claims 11, 19, 26 and 51.

For instance, Arthan et al. teaches that the destination system 2 receives the active public key from the central system 5. Further, the central system 5 outputs the active private key to the source system 1 for use in encrypting data from the source system 1, and the central system 5 does not use the output private key for authentication. Accordingly, the first public key does not have a corresponding first private key stored on the central system 5, where the first public key is used for authentication of the central system 5. Similarly, the source system 1, which uses the first private key for encrypting data sent to the destination system, does not send any public keys to any other devices. Accordingly, there is no teaching or suggestion of receiving the first public key or the second public key from the source system 1.

Furthermore, neither Kurn et al. nor Hansmann et al. include any teachings or suggestions to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "receiving a first public key from a mobile user device **wherein the first public key has a corresponding first private key stored on the mobile user device**; receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication; **using the first public key for authentication** of the mobile user device; and **using the second public key for authentication if the first public key fails**," as recited in independent claim 11, and as similarly recited in independent claims 19, 26 and 51, and these differences between claims 11, 19, 26 and 51 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 11, 19, 26 and 51.

Furthermore, the nonobviousness of independent claims 11, 19 and 26 precludes a rejection of claims 12, 13, 20, 21, 27 and 28, which depend therefrom, because a dependent

claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 12, 13, 20, 21, 27 and 28, in addition to the rejection to independent claims 11, 19, 26 and 51.

Claims 57-68

Independent claim 57 recites "re-creating a second private key **at a mobile user device that has no access to a first private key associated with the second private key**, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; **outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device**; and using the second private key for authentication of the mobile user device." Independent claims 61 and 65 also include similar recitations.

The rejection of claims 57, 61 and 65 is dependent upon the same arbitrary modification of Arthan et al. as asserted against all the previously discussed independent claims. Specifically, the Office Action takes the position that the source system 1 and the central system 5 are integrated into a single system or device. *See Office Action* at p. 2. However, as noted above with regards to independent claim 50, the characterization of Arthan et al. as teaching that the central system 5 can be readily integrated into the source system 1, and that such integration would have been obvious is well beyond the realm of what Arthan et al. reasonably and fairly teaches, and is contrary to the explicit teachings of Arthan et al. Indeed, the only motivation to arbitrarily modify Arthan et al. in the manner asserted is strictly based on impermissible hindsight.

For instance, there is no teaching or suggestion that the central system 5 is or can be implemented as a physically separate node of the source system 1. Instead, throughout the disclosure, Arthan et al. actually depicts and suggests that the source system 1 and the central system 5 are separate and distinct entities. Furthermore, the mischaracterization of the central system 5 as being integrated into the source system 1 renders various teachings in Arthan et al.

as obsolete and meaningless. Indeed, the arbitrary modification of Arthan et al. is based solely on Applicants' disclosure, as a result of statutorily prohibited hindsight.

Additionally, Arthan et al., when considered as a whole, teaches away from the modifications proposed by the Office Action. For instance, Arthan et al. expressly requires that the operators 3 of the source system 1 are not authorized to handle the private key. *Arthan et al.* at col. 2, lines 35-38. On the other hand, the security officer 6 is suggested as being authorized to handle the private key in order to manually deliver and install the keys, and to change the various versions of the private key. *Id.* at col. 1, lines 46-50; and col. 5, lines 7-10. Thus, the security officer 6 cannot become an operator 3 of the source system 1. Therefore, the central system 5, which the security officer 6 uses to manage the keys, cannot be arbitrarily transformed into a part of the source system 1 without departing from the express requirements of the Arthan et al. disclosure.

Furthermore, the fact that Arthan et al. suggests that the security officer 6, who uses the central system 5 to manage the private keys, cannot be an operator 3 of the source system 1 is evidence supporting the conclusion that the proposed modification of Arthan et al. would not be obvious, but would instead be patentable. That is, combining the central system 5 with the source system 1 such that the user of the integrated device may both operate the device and manage keys is expressly contrary to the understanding and expectations of Arthan et al., and such modifications are patentable when they show insight that was contrary to the understanding and expectations of the art. *See MPEP* § 2144.04(V)(B); and *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983).

Finally, when Arthan et al. is characterized according to what is reasonably and fairly taught by the disclosure as a whole, Arthan et al. fails to teach or suggest all of the features recited by independent claims 57, 61 and 65, since neither of the separate and distinct entities from among the source system 1, destination system 2 or central system 5 are taught or suggested by Arthan et al. as including all of the features recited by independent claims 57, 61 and 65.

For instance, as noted above regarding independent claim 50, the central system 5 of Arthan et al. generates an active private and public key pair and a spare private and public key pair. See *Arthan et al.* at col. 3, lines 38-41; and col. 4, lines 15-20. The central system 5 then

outputs the active private key to the source system 1, and the active public key and spare public key to the destination system 2. *Id.* at col. 3, lines 25-41; col. 4, lines 15-20. It appears from Arthan et al. that the central system 5 securely stores the spare private key for future deployment to the source system 1. *Id.* at col. 4, lines 25-32.

Such a central system 5 is contrary in at least some respects to the recitations in independent claim 57. In claim 57, the **retained** private key is used for authentication prior to using the output private key. In the central system 5, the **output** private key is used by the source system 1 prior to using the stored spare private key.

In addition, the central system 5 that creates the first and second key pairs does not appear to actually use any of the keys for authentication of the central system 5. Instead, it just generates the keys and then sends them off to other devices for use by these other devices. This is contrary to claim 57, where the second private key is re-created at the mobile user device and the third private and public keys are created at the mobile user device, and the retained second private key is used for authentication of the mobile user device.

Arthan et al. also does not teach or suggest the source system 1 or the destination system 2 as performing any steps relating to outputting one private key while retaining another private key and using the retained private key for authentication. Accordingly, Arthan et al. fails to teach or suggest "**outputting the third private key** from the mobile user device such that it is not stored on the mobile user device **while retaining the second private key** in the mobile user device," and "**using the second private key** for authentication of the mobile user device **before using the third private key**," as recited in independent claim 57.

Furthermore, neither Kurn et al. nor Hansmann et al. include any teachings or suggestions to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "**re-creating a second private key at a mobile user device** that has no access to a first private key associated with the second private key, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; **outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at**

the mobile user device; and **using the second private key for authentication** of the mobile user device **before using the third private key**," as recited in independent claim 57 and as similarly recited in independent claims 61 and 65, and these differences between claims 57, 61 and 65 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 57, 61 and 65.

Furthermore, the nonobviousness of independent claims 57, 61 and 65 precludes a rejection of claims 58-60, 62-64 and 66-68, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 58-60, 62-64 and 66-68, in addition to the rejection to independent claims 57, 61 and 65.

Claims 10 and 15

The Office Action rejected claims 10 and 15 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."), in view of U.S. Publication No. 2002/0018570 (hereinafter "Hansmann et al."), and further in view of Official Notice. These rejections are respectfully traversed in their entirety.

Claims 10 and 15 depend from claims 1 and 14, respectively. As noted previously, the combination of Arthan et al., Kurn et al., and Hansmann et al. fail to teach or suggest all of the limitations of independent claims 1 and 14. The nonobviousness of independent claims 1 and 14 precludes a rejection of claims 10 and 15, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 10 and 15.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: June 22, 2011

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502